430 Rec'd PCT/PTO 15 FEB 2000

FORM PTO-1390 (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: 3220-60866

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/485759 Unknown

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US98/17321	21 August 1998	22 August 1997

TITLE OF INVENTION: HIDING OF ENCRYPTED DATA

APPLICANT(S) FOR DO/EO/US: GLOGAU, Jordan J.; DELP, Edward J., III; WOLFGANG, Raymond B.; LIN, Eugene Ted

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [ ] This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] has been transmitted by the International Bureau.
   c. [X] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [X] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [X] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [X] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). Two in Counterpart.
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    a. Copies of the PCT International Search Report and Each Reference Cited Therein
    b. Copy of the PCT International Preliminary Examination Report
    c. Statement Claiming Small Entity Status (37 CFR 1.9(f) & 1.27(d))--NonProfit Organization

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
Unknown 09/485759	PCT/US98/17321	3220-60866

17. [XX] The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $970.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $840.00		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $760.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $670.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ -0-	

CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total claims	29	- 20 =	9	X $18.00	$ 162.00	
Independent claims	5	- 3 =	2	X $78.00	$ 156.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+ $260.00	$ -0-	

TOTAL OF ABOVE CALCULATIONS =	$ 1158.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).	$ 579.00	
SUBTOTAL =	$ 579.00	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +	$ -0-	
TOTAL NATIONAL FEE =	$ 579.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +	$ -0-	
TOTAL FEES ENCLOSED =	$ 579.00	
	Amount to be: refunded	$
	charged	$

a. [XX] A check in the amount of $ 579.00 to cover the above fees is enclosed.

b. [ ] Please charge my Deposit Account No. ______________ in the amount of $____________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [X] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 10-0435. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO

LAMMERT, Steven R.
BARNES & THORNBURG
11 South Meridian Street
Indianapolis, IN 46204
US

Steven R. Lammert (signature)
SIGNATURE

Steven R. Lammert
NAME

27653
REGISTRATION NUMBER

BARNES & THORNBURG

11 South Meridian Street
Indianapolis, Indiana 46204
(317) 236-1313

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Group:	Unknown
Attorney Docket:	3220-60866
Applicant:	GLOGAU, Jordan J.; DELP, Edward J. III; WOLFGANG, Raymond B.; LIN, Eugene Ted
Invention:	HIDING OF ENCRYPTED DATA
U.S. Serial No:	Unknown
International. Serial No:	PCT/US98/17321
International Filing Date:	21 August 1998 (21.08.98)
Earliest Priority Date:	22 August 1997 (22.08.97)

Certificate Under 37 CFR 1.10

Express Mail Label No. EM466245407US

Date of Deposit: 15 February 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service's "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231

Mary Jean Eskridge
Typed or Printed Name of Person Mailing Paper or Fee

Mary Jean Eskridge
Signature of Person Mailing Paper or Fee

FIRST PRELIMINARY AMENDMENT

Attention: DO/EO/US
Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Preliminary to the examination of the above-identified national patent application submitted herewith, applicants request entry of the following amendments.

In the Description

After the title, please insert the following paragraph:

--Cross-References to Related Applications

This application is a U.S. national application of international application serial No. PCT/US98/17321 filed August 21, 1998, which claims priority to U.S. provisional application serial No. 60/056,724 filed August 22, 1997.--

REMARKS

This Preliminary Amendment is being submitted to indicate the relationship of the subject U.S. national application to previously filed applications as required under 37 C.F.R. 1.78. With the entry of the foregoing amendments, the application is believed to be in condition for examination and allowance. Consideration of the claims, leading to their allowance and passage of the application to issuance, is respectfully requested.

Respectfully submitted,

Steven R. Lammert

Steven R. Lammert
Atty. Reg. No. 27653
Attorney for Applicants

SRL/mje/300156
Indianapolis, Indiana 46204
(317) 231-7258

PTO/SB/11 (12-97)
Approved for use through 9/30/00 OMB 0651-0031
Patent and Trademark Office; U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(d))--NONPROFIT ORGANIZATION

Docket Number (Optional) 3220-60866

Applicant ~~XXXXXX~~, or Identifier: Jordan J. GLOGAU; Edward J. DELP III; Raymond B. ~~WOLFGANG; Eugene Ted LIN~~

Application ~~XXXXXX~~ No.: ____

Filed ~~XXXXXX~~: ____

Title: HIDING OF ENCRYPTED DATA

I hereby state that I am an official empowered to act on behalf of the nonprofit organization identified below:

NAME OF NONPROFIT ORGANIZATION PURDUE RESEARCH FOUNDATION

ADDRESS OF NONPROFIT ORGANIZATION 1021 Hovde Hall, Room 307
West Lafayette, IN 47907-1021

TYPE OF NONPROFIT ORGANIZATION:

☐ UNIVERSITY OR OTHER INSTITUTION OF HIGHER EDUCATION

☒ TAX EXEMPT UNDER INTERNAL REVENUE SERVICE CODE (26 U.S.C. 501(a) and 501(c)(3))

☐ NONPROFIT SCIENTIFIC OR EDUCATIONAL UNDER STATUTE OF STATE OF THE UNITED STATES OF AMERICA
(NAME OF STATE ____)
(CITATION OF STATUTE ____)

☐ WOULD QUALIFY AS TAX EXEMPT UNDER INTERNAL REVENUE SERVICE CODE (26 U.S.C. 501(a) and 501(c)(3)) IF LOCATED IN THE UNITED STATES OF AMERICA

☐ WOULD QUALIFY AS NONPROFIT SCIENTIFIC OR EDUCATIONAL UNDER STATUTE OF STATE OF THE UNITED STATES OF AMERICA IF LOCATED IN THE UNITED STATES OF AMERICA
(NAME OF STATE ____)
(CITATION OF STATUTE ____)

I hereby state that the nonprofit organization identified above qualifies as a nonprofit organization as defined in 37 CFR 1.9(e) for purposes of paying reduced fees to the United States Patent and Trademark Office regarding the invention described in:

XX the specification filed herewith with title as listed above.
☐ the application identified above.
☐ the patent identified above.

I hereby state that rights under contract or law have been conveyed to and remain with the nonprofit organization regarding the above identified invention. If the rights held by the nonprofit organization are not exclusive, each individual, concern, or organization having rights in the invention must file separate statements as to their status as small entities and that no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization having any rights in the invention is listed below:

XX no such person, concern, or organization exists.
☐ each such person, concern, or organization is listed below.

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

NAME OF PERSON SIGNING Bruce L. Pershing

TITLE IN ORGANIZATION OF PERSON SIGNING Investment Officer and Secretary

ADDRESS OF PERSON SIGNING 1063 Hovde Hall, West Lafayette, IN 47907-1063

SIGNATURE Bruce L Pershing DATE February 2, 2000

DATA HIDING

Field of the Invention

The present invention relates to methods and apparatus for hiding data within a digital signal, and particularly for concealing information within multimedia signals such as digital image, audio, or video signals. More particularly, the present invention relates to methods and apparatus for embedding and retrieving information into and out of a digital signal used in multimedia applications while minimizing the effect on the multimedia application of the digital signal.

Background and Summary of the Invention

The art of concealing information has existed for millennia and is one to which computers have been readily adapted. It is known, for example, to use computers for encrypting data using various symmetric and asymmetric cryptographic schemes such as the Data Encryption Standard (DES) and RSA encryption, and cryptographic software packages such as PGP (Pretty Good Privacy). Another technique for concealing information for which computers are used is data hiding or steganography, in which the existence of certain information is concealed within a carrier communication. In contrast to cryptography, where it is a goal to make a message undecipherable regardless of its detection, with steganography it is a goal to hide the very existence of the hidden message. An example of a known steganography technique using computers is to embed a digital watermark into a digital image.

According to the present invention, a method of hiding data is provided. A message to be hidden and an encrypting sequence are provided along with a carrier signal that conveys information (unrelated to the message). An encrypted message is generated based on the message and the encrypting sequence. The encrypted message is embedded into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

In preferred embodiments, the carrier signal is a digital image, and the first portion of the carrier signal is an LSB plane of the digital image. The digital image has a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first

color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

According to another aspect of the invention, the carrier signal is transmitted to a receiving location. The encrypted message is extracted and from the carrier signal and deciphered at the receiving location. In preferred embodiments, the encrypted sequence is generated based on an encrypting key. The encrypted message is generated by performing an exclusive-OR of the message with the encrypting sequence.

According to yet another aspect of the invention, a method of data hiding is provided in which an encryption key and a carrier signal that conveys information unrelated to the encryption key are supplied. An encryption sequence based on the encryption key is generated. The encryption sequence is embedded into the carrier signal.

In preferred embodiments, the encryption key is a public key for an asymmetric encryption algorithm. The carrier signal can be a signal such as a digital image, digital audio, or digital video. The encryption sequence is substantially random, and can be generated based on a linear feedback shift register. The encryption sequence is embedded into the carrier signal by performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

According to other aspects of the invention, the carrier signal including the embedded encryption sequence is transmitted to a receiving location. The encryption sequence is extracted from the composite signal at the receiving location. The encryption sequence is decrypted to obtain the encryption key. The encryption key is used to generate an encrypted message at the receiving location, and the encrypted message is transmitted from the receiving location.

According to yet another aspect of the invention, a method of data hiding is provided. An encrypted message is embedded into a first portion of a carrier signal and message extraction information is embedded into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

In preferred embodiments, the encrypted message is embedded by performing an exclusive-OR of the encrypted message with the first portion of the carrier signal. The message extraction information is embedded by performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal. The

first and second portions of the carrier signal can be first and second bit-planes of a digital image.

According to still another aspect of the invention, a method of exchanging data hidden in a carrier signal is provided. A signal including hidden data is generated by transforming a carrier signal from a first domain into a second domain. A message is embedded into the carrier signal in the second domain. The carrier signal is transformed back from the second domain to the first domain. The signal including hidden data is sent to a receiving location. The message is obtained from the signal including hidden data at the receiving location by transforming the signal including hidden data into the second domain and extracting the message.

In preferred embodiments, the message is encrypted prior to generating the signal including hidden data. The message is decrypted after obtaining the message from the signal including hidden data.

According to still yet another aspect of the invention, a data hiding apparatus is provided. An encryption sequence generator generates an encryption sequence based on an encrypting key. An encrypted message generator generates an encrypted message based on the encryption sequence and an input message. An encrypted message embedder embeds the encrypted message into a carrier signal.

In preferred embodiments, the encryption sequence generator generates a substantially random encryption sequence. The encrypted message embedder performs an exclusive-OR of the encrypted message with a portion of the carrier signal. The encrypted message embedder replaces a first LSB plane of a digital image with information based on a second LSB plane of the digital image and performs an exclusive-OR of the encrypted message with the second LSB plane of the digital image. The encrypted message generator performs an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

Additional features of the invention will become apparent to those skilled in the art upon consideration of the following detailed description of the preferred embodiments exemplifying the best mode of carrying out the invention as presently perceived.

Brief Description of the Drawings

Fig. 1 is a block diagram of two computer systems connected over a network, each computer system configured with a processor and memory for implementing embodiments of the present invention;

Fig. 2 is a flow chart showing a method according to the present invention for hiding data within an image for transmission over a network;

Fig. 3 is a high level block diagram showing a technique for embedding encrypted information into a carrier signal;

Fig. 4 is a more detailed block diagram similar to Fig. 3 showing a similar, more specific technique for embedding encrypted information into a carrier signal;

Fig. 5 is a stylized representation of a message format containing embedded, hidden information;

Fig. 6 is a stylized representation similar to Fig. 5 of an alternative message format; and

Fig. 7 is a flow chart showing an alternative method according to the present invention for hiding data within an image for transmission over a network.

Detailed Description of the Illustrative Embodiments

The present invention lends itself to implementation in a conventional computer network 10 as shown in Fig. 1. Computer network 10 illustratively includes computer systems 12, 18 connected through a series of network communication devices 14, 16, 20 (e.g., modems, transceivers, etc.) for communication over a network 22 such as the standard telephone lines, or the Internet or World Wide Web. Computer systems 12, 18 are illustratively personal computers and each includes basic elements such as a processor 26, 32, memory 28, 34, storage device 30, 36, and display 31, 38. Computer systems 12, 18 can also include optional peripheral devices such as removable storage device 40 (e.g., a CD-ROM or 3½ inch disk drive).

An exemplary method of data hiding according to the present invention that is suitable for carrying out on computer network 10 is shown in Fig. 2. Although the present invention is disclosed in the context of certain embodiments discussing digital images, other digital signals, such as digital audio or video signals, are also within the scope of the invention.

According to the method of Fig. 2, an image is used to transport and exchange data that is embedded in the image itself and that cannot be perceived by the human eye. An appropriate analogy is that the image acts as an envelope, with the embedded data transmitted with the image being equivalent to a letter contained within the envelope. Conventional encryption such as PGP or RSA is used to enhance security of the embedded data. The security is improved because the encrypted data is hidden within the image and therefore cannot be recognized as such. This allows for secure data communication and exchange over an insecure transmission channel.

In step 50 an original digital image is obtained. A secret message that is desired to be embedded into the image is generated in step 52. A message encrypting key is used in step 54 to generate an encryption sequence. The message encrypting key can be a seed value for use in generating an m-sequence from a linear feedback shift register as discussed in more detail below, although it is understood that any suitable message encrypting algorithm can be used. As also discussed below, the message encrypting key will ultimately be used by the recipient of the image embedded with the secret message.

In step 56 the secret message from step 52 is encrypted with the encryption sequence from step 54 to create an encrypted message. The encrypted message is then embedded into the image in step 58. There are many methods to embed the encrypted message into the image such as the method discussed below, but, again, it is understood that other suitable methods can be used.

The image with the embedded message is then made available such as on a public network as shown in step 60. Finally, if the secret message from step 52 is actually information that is not desired to be kept secret, such as a public key for an asymmetric encryption algorithm, then the encryption key from step 54 is also made available on the public network as shown in steps 62, 64. This allows for third parties to extract the message from the image. Thus, for example, the message can be a public encryption key that is hidden within the image but that is readily available to a party that has knowledge of the fact that the hidden message exists. This provides a convenient way of exchanging information, such as allowing an individual to make a public encryption key available over the World Wide Web by posting it within an image on a Web site, while still concealing the information from the casual observer.

It is useful at this point to provide some preliminary definitions before discussing a specific implementation of the method of Fig. 2. The symbol $\oplus$ denotes a bit exclusive-OR function (equivalently, modulo-2 addition). Table 1 illustrates the exclusive-OR function:

Table 1

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

A digital image is typically represented with a two dimensional array of pixel values. If A is the array of pixel values, then A(x,y) denotes the pixel value in the x-th column of the y-th row of the array. Each index x,y begins at zero, and by convention the origin is at the upper-left corner with positive coordinates going rightwards and downwards, although this convention is somewhat arbitrary.

For labeling purposes, it will be assumed that the digital image is a 24-bit RGB image with pixel values ordered as shown in Table 2: xx

Table 2

MSB																								LSB
Red								Green								Blue								
23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
R7	R6	R5	R4	R3	R2	R1	R0	G7	G6	G5	G4	G3	G2	G1	G0	B7	B6	B5	B4	B3	B2	B1	B0	

Thus, bits 16-23 refer to the red component, bits 8-15 refer to the green component, and bits 0-7 refer to the blue component for any given pixel value. For example, $I_{G0}(x,y)$ refers to the least-significant bit of the green component of the (x,y)-pixel in the image I. Since bit G0 is equivalent to bit 8, $I_{G0}(x,y)$ is equivalent to $I_8(x,y)$. As with the array convention, this labeling convention is somewhat arbitrary.

An m-sequence is a pseudo-random sequence of binary digits (bits). m-sequences have good statistical properties and can be generated by linear feedback shift registers (configured appropriately as is known in the art). Knowing the size (number of bits), structure (the feedback configuration), and initial fill (the initial contents of each bit) of the shift register allows the reconstruction of the entire m-sequence. The m-sequences here illustratively are generated by a 96-bit m-sequence generator. If the structure and size of the shift register are known (as would be the case with this embodiment), and if a consecutive portion of the m-sequence equal to twice the shift register size is also known,

the initial fill used to generate the sequence can be determined. In this embodiment the initial fill is used as the key that generates the m-sequence. In this way, the key can be determined from the sequence itself by techniques known to those skilled in cryptography.

When embedding a message into a carrier signal, the order in which pixel operations are performed may be an important consideration. A sequence function z(i) is defined to provide a one-to-one mapping from i->(x,y), where i is an ordinal number and (x,y) refers to coordinate values in an image. The ordinal i ranges from zero to N-1, where N is the total number of pixels in the image. Given a sequence function z(i), one can compute z(0), z(1), z(2), etc., to obtain a sequence of pixel coordinates (x_1,y_1), (x_2,y_2), etc. As an example, z(i) = (i mod ImageWidth, $\lfloor$i / ImageWidth$\rfloor$) denotes a sequence beginning at the origin and proceeding in a row-by-row fashion.

Given these preliminary definitions, an implementation corresponding to the illustrative method of Fig. 2 of embedding a message into an image is shown by the block diagram in Fig. 3. Input signals are a source image 66 (obtained in step 50), an unencrypted message 68 (generated in step 52), and an encrypting key 70 (used in step 54). Message 68 and encrypting key 70 are processed by an encrypted message generator 76 to create an encrypted message signal 72. Encrypted message 72 is an input along with source image 66 into composite signal generator 78, which creates a composite signal 74 containing source image signal 66 embedded with encrypted message 72.

Composite signal generator 78 illustratively embeds encrypted message 72 into the least-significant bit in the green plane $I_{G0}(x,y)$ of source image 66 to create a new least-significant green bit-plane $I'_{G0}(x,y)$ of composite signal 74. In order subsequently to extract encrypted message 72 from composite signal 74 (I') it will be necessary to know the original values of $I_{G0}(x,y)$ from source image 66. This can of course easily be accomplished by making the original, unmodified image signal 66 available. Composite signal generator 78, however, eliminates the requirement of using original image signal 66 by encoding the original $I_{G0}(x,y)$ into the least-significant red bit-plane $I'_{R0}(x,y)$ of composite signal 74 as discussed below. Thus, in order to extract the embedded encrypted message 72, only composite signal 74 and the encrypting key 70 are needed.

In order to use the method of Figs. 2 and 3 both a sender and receiver of composite signal 74 will need an m-bit shift register with identical feedback configurations and a well-defined ordering function z(i) for any arbitrary image. The following steps

describe the generation of the composite signal 74 (also referred to as public image I') from original signal 66 (also referred to as original image I), unencrypted message 68 (illustratively a public encryption key, also referred to as K_{PUB}), and encrypting key 70 (also referred to as K_I). As intimated above, encrypting key 70 (K_I) is the initial fill of the m-sequence generator.

In order to generate I', I' is initially set to be an exact copy of I. I' is then traversed in order z(i) and the red and green least-significant bit planes are set to:

$$I'_{R0}(z(i)) = I'_{G0}(z(i)) \oplus \text{m-seq}(2i)$$

$$I'_{G0}(z(i)) = K_{PUB}(i) \oplus I'_{G0}(z(i)) \oplus \text{m-seq}(2i+1)$$

where $K_{PUB}(i)$ refers to the I-th bit of K_{PUB}, and m-seq(j) refers to the j-th bit in the m-sequence using K_I as the initial fill. With these two equations, information on portion 2 of the image (the green LSB plane) is first placed in portion 1 of the image (the red LSB plane). Then, the message is embedded in portion 2.

To recover K_{PUB} it is only necessary to have the composite signal or public image I' and the encrypting key K_I. For each pixel in I' and in the order z(i), the first step is to extract $I_{G0}^*(z(i))$ by using the least-significant red bit plane and the m-sequence:

$$I_{G0}^*(z(i)) = I'_{R0}(z(i)) \oplus \text{m-seq}(2i)$$

$I_{G0}^*(z(i))$ is identical to $I_{G0}(z(i))$ if there are no errors in I'. Then the i-th bit of $K_{PUB}(i)$ is computed by using $I_{G0}^*(z(i))$:

$$K_{PUB}^*(i) = I'_{G0}(z(i)) \oplus I_{G0}^*(z(i)) \oplus \text{m-seq}(2i+1)$$

Thus, given K_I, it is possible to reconstruct the same m-sequence used to generate I'. Thus, if no errors occur K_{PUB}^* should be identical to K_{PUB}. Thus, the method of the invention provides for including within the image both the message that is embedded or encrypted in the image as well as the information needed to extract or decrypt the message from the image.

A more specific method corresponding to an implementation of the method of Figs. 2 and 3 is shown Fig. 4. The same input signals are used, that is, source image 66 (I), message 68 (here, Q instead of K_{PUB}), and encrypting key 70 (K_I) are used. The primary refinement in the method of Fig. 4 as compared with Fig. 3 is an encoding process to handle varying length messages 68.

Message 68, which in the example of Fig. 3 was a public encryption key for use in an asymmetric cryptography system, can more generally simply be a collection of bits intended to be encrypted and is referred to here as Q. The length (i.e., the total number of bits) of Q is denoted $|Q|$. The i-th bit of the message Q is denoted Q(i), where the bits are numbered from 0 to $|Q|-1$.

Message 68 (Q) is an input signal to message generator 82 which has as a second input the output from a random noise generator 84. Random noise generator 84 illustratively is also a 96-bit m-sequence generator using an initial fill of a computer system time value, although other suitable random signal generators can be used. Encrypting key 70 (K_I) is an input signal (initial fill) to an m-sequence generator 80 that illustratively is the same as random noise generator 84, which then generates as an output an encrypting sequence 86.

Unless the message 68 (Q) will always be the same length (in bits) and that length is the number of pixels in the source image, it will not be possible to embed Q directly onto source image 66 (I). It is therefore necessary to encode additional information that will enable subsequent extraction of messages Q of varying sizes from composite signal 74 (I'). Thus, the message 88 to be encoded onto image 66 (I) is generated by message generator 82 with special properties and is denoted Q' to show that it is derived from Q.

Q' has the following properties. For any given source image I, regardless of what message Q is being encoded, the size of a message Q' is the same as the total number of pixels in image I (that is, $|Q'|$ = # pixels in I). The bits of message Q' are labeled according to standard convention, that is, the first bit (or the left-most bit if Q' is viewed as an ordered bit stream from left to right as shown in Fig. 5) is numbered zero. Thus the bits of Q' are numbered from zero to $|Q'|-1$.

The structure of Q' is shown in Fig. 5. All bits except the last sixty-four form a data area 92. The last sixty-four bits consist of two thirty-two bit words (StartPos

and Length, in that order), which form a Trailer. Data area 92 includes data bits 98 that correspond to the message Q itself, and random bits 97, 99 that help hide the location of Q (bits 98) within Q'. As part of the encoding process, message generator 82 computes the length of message Q and stores its value in the final 32 bits 94 of the Trailer. The value of the length is not directly encoded and instead a value congruent (actual length modulo Data Area size) is placed in the 32-bit word. It is trivial to recover the length from this encoded value.

Starting position 94 describes the location within data area 92 where the bits of the message Q reside. Message generator 82 randomly chooses a place 98 to store Q and populates all other bits of unused portions 97, 99 in data area 92 with random noise generated by random noise generator 84. Thus, Q can be anywhere in data area 92. Including noise for portions 97, 99 of data area 92 unused by message Q improves security of data embedded within I because the noise increases the difficulty of recognizing the existence or location of Q within the data area.

The encoding of each bit of message Q' is encoded onto image I on a one-bit per one-pixel basis using an exclusive-OR as discussed above for the method of Fig. 3. First, the output of m-sequence generator 80 (with K_1 as a seed value) is used to encrypt Q' in encrypter 90. Next, the encrypted Q' is embedded onto the LSB green plane I_{G0}. Encrypted message Q is subsequently extracted from Q' by locating its starting position and length from the trailer. The extracted Q is then decoded as discussed above.

Further implementation steps can be taken to increase security for message Q'. Random number generator 84 and m-sequence generator 80 can be different. Even if both use 96-bit m-sequence generators, this can be achieved simply by changing the feedback coefficients. Moreover, the message length 94 in the trailer can be relocated to data area 92 as shown in Fig. 6. This relocation will limit the ability of an attacker to take advantage of a known size of message Q.

Another way to provide for security of data hidden within a carrier image is shown by the method of Fig. 7. In step 102 the carrier image is transformed from a first domain to a second domain. For example, a typical RGB image that is considered to be represented in a spatial domain can be transformed using a discrete cosine transform. A message is then embedded into the transformed carrier image in step 104, using any appropriate technique for embedding a message onto a carrier signal. An example of a

transformed image into which a message can be embedded would be a JPEG image. If desired, the message can also be pre-encrypted before being embedded into the transformed image to further improve security. The image is then transformed back into the first domain in step 106 and made available for access by third parties in step 108.

For a third party to extract the message the steps are essentially reversed. First the image is copied by the third party in step 110, and it is then transformed into the second domain in step 112 using the same transform performed in step 106. Finally, the message is extracted in step 114, again, using any appropriate technique that corresponds to the technique used in step 104 for originally embedding the message. If the message was pre-encrypted then another decryption step (not shown) will be necessary.

Encrypted messages relying on the use of encryption keys are used in the methods discussed above. For example, if a pre-encrypted message is embedded into an image, then the recipient will need a key to decrypt the message. A technique for providing for secure exchanges of encrypted data such as encryption keys that is known in the art is the use of a trusted third party. The trusted third party essentially acts as a secure broker in exchanging data between two other parties. It is within the scope of this invention to exchange information, such as encryption keys, by use of a trusted third party.

Although the invention has been described in detail with reference to certain illustrated embodiments, variations and modifications exist within the scope and spirit of the present invention as described and defined in the following claims.

CLAIMS:

1. A method of data hiding comprising the steps of:

providing a message;

providing an encrypting sequence;

generating an encrypted message based on the message and the encrypting sequence;

providing a carrier signal that conveys information unrelated to the encrypted message; and

embedding the encrypted message into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

2. The method of claim 1, wherein the carrier signal is a digital image.

3. The method of claim 2, wherein the first portion of the carrier signal is an LSB plane of the digital image.

4. The method of claim 1, further comprising the step of embedding the first portion of the carrier signal into a second portion of the carrier signal.

5. The method of claim 4, wherein the carrier signal is a digital image having a plurality of color planes, the first portion of the carrier signal is an LSB plane of a first color plane, and the second portion of the carrier signal is an LSB plane of a second color plane.

6. The method of claim 1, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location.

7. The method of claim 1, wherein the step of generating an encrypted message includes generating the encrypting sequence based on an encrypting key and performing an exclusive-OR of the message with the encrypting sequence to generate the encrypted message.

8. The method of claim 7, further comprising the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location, and decrypting the encrypted message at the receiving location based on the encrypting key.

9. The method of claim 1, wherein the step of providing a message comprised of providing a pre-encrypted message.

10. The method of claim 9, further comprising the step of exchanging an encryption key for decrypting the pre-encrypted message using a trusted third party.

11. A method of data hiding comprising the steps of:

providing an encryption key;

generating an encryption sequence based on the encryption key;

providing a carrier signal that conveys information unrelated to the encryption key; and

embedding the encryption sequence into the carrier signal.

12. The method of claim 11, wherein the encryption key is a public key for an asymmetric encryption algorithm.

13. The method of claim 11, wherein the carrier signal is selected from the group comprising digital images, digital audio, and digital video.

14. The method of claim 11, wherein the encryption sequence is substantially random.

15. The method of claim 14, wherein the encryption sequence is generated based on a linear feedback shift register.

16. The method of claim 11, wherein the step of embedding the encryption sequence includes performing an exclusive-OR of the encryption sequence with a portion of the carrier signal.

17. The method of claim 11, further comprising the steps of transmitting the carrier signal including the embedded encryption sequence to a receiving location, extracting the encryption sequence from the composite signal at the receiving location, and deciphering the encryption sequence to obtain the encryption key at the receiving location.

18. The method of claim 17, further comprising the steps of encrypting a message using the encryption key to generate an encrypted message at the receiving location and transmitting the encrypted message from the receiving location.

19. A method of data hiding comprising the steps of:

embedding an encrypted message into a first portion of a carrier signal; and

embedding message extraction information into a second portion of the carrier signal for extracting the encrypted message from the first portion of the carrier signal.

20. The method of claim 19, wherein the step of embedding an encrypted message includes performing an exclusive-OR of the encrypted message with the first portion of the carrier signal.

21. The method of claim 20, wherein the step of embedding message extraction information includes performing an exclusive-OR of the first portion of the carrier signal with the second portion of the carrier signal.

22. The method of claim 21, wherein the first and second portions of the carrier signal are first and second bit-planes of a digital image.

23. A method of exchanging data hidden in a carrier signal comprising the steps of:

generating a signal including hidden data by transforming a carrier signal from a first domain into a second domain, embedding a message into the carrier signal in the second domain, and transforming the carrier signal back from the second domain to the first domain;

sending the signal including hidden data to a receiving location; and

obtaining the message from the signal including hidden data at the receiving location by transforming the signal including hidden data into the second domain and extracting the message.

24. The method of claim 23, further comprising the steps of encrypting the message prior to generating the signal including hidden data and decrypting the message after obtaining the message from the signal including hidden data.

25. A data hiding apparatus comprising:

an encryption sequence generator configured to generate an encryption sequence based on an encrypting key;

an encrypted message generator configured to generate an encrypted message based on the encryption sequence and an input message; and

an encrypted message embedder configured to embed the encrypted message into a carrier signal.

26. The method of claim 25, wherein the encryption sequence generator is configured to generate a substantially random encryption sequence.

27. The method of claim 25, wherein the encrypted message generator is configured to perform an exclusive-OR of the input message with the encrypting sequence to generate the encrypted message.

28. The method of claim 25, wherein the encrypted message embedder is configured to perform an exclusive-OR of the encrypted message with a portion of the carrier signal.

29. The method of claim 28, wherein the encrypted message embedder is configured to replace a first LSB plane of the digital image with information based on a second LSB plane of the digital image and to perform an exclusive-OR of the encrypted message with the second LSB plane of the digital image.

DATA HIDING

Abstract of the Disclosure

A method of data hiding includes providing a message (68), providing an encrypting sequence (86), and generating an encrypted message (72) based on the message and the encrypting sequence. A carrier signal (66) that conveys information unrelated to the encrypted message is provided, and the encrypted message is embedded (78) into the carrier signal by performing an exclusive-OR of the encrypted message with a first portion of the carrier signal.

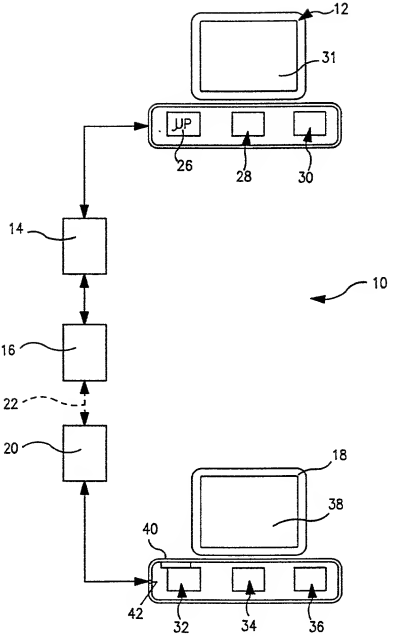

FIG. 1

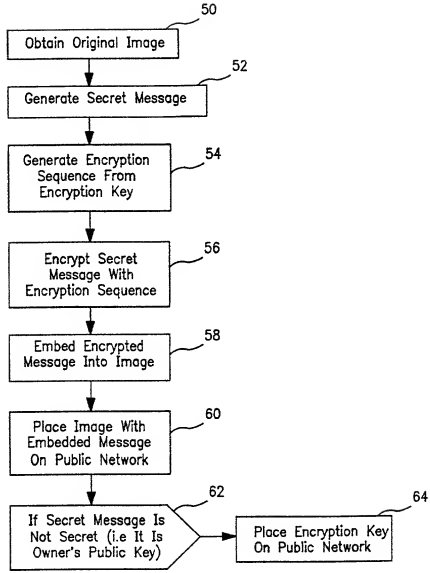

FIG. 2

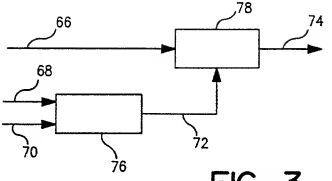

FIG. 3

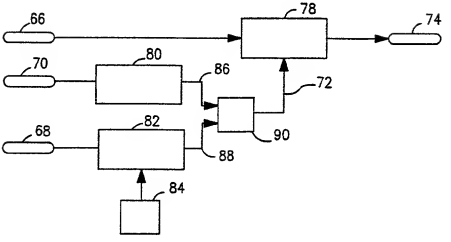

FIG. 4

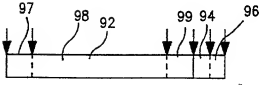

FIG. 5

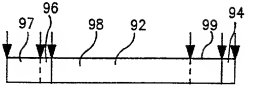

FIG. 6

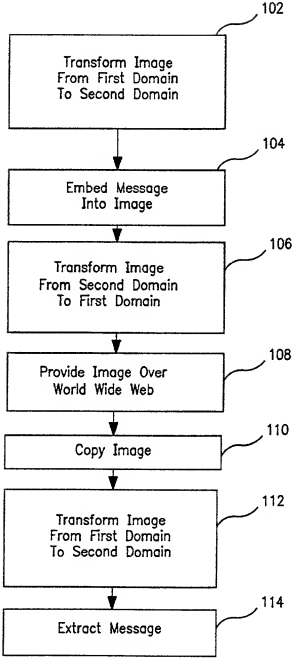

FIG. 7

Express Mail No.: EM466245407US

Attorney Docket No.: 3220-P-97064.00.US

DECLARATION AND POWER OF ATTORNEY -- PATENT APPLICATION

As a below named inventor, I hereby declare that I believe I am the original, first and sole inventor (*if only one name is listed below*) or an original, first and joint inventor (*if plural names are listed below*) of the subject matter which is claimed and for which a patent is sought in the application entitled:

DATA HIDING ______________________________, the specification of which

(*check one*)

_______ is attached hereto

XX was filed on 21 August 1998 (21.08.98) as

United States Application Serial No. ______________________ or

PCT International Application No. PCT/US98/

and was amended on ______________________

(if applicable)

I hereby declare that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to herein.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate on which priority is claimed (as listed below) and I have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(b) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)
60/056,724	(22.08.97) 22 August 1997	Abandoned

I hereby appoint William R. Coffey, Reg. No. 24023; Jerry E. Hyland, Reg. No. 20904; Richard D. Conard, Reg. No. 27321; Steven R. Lammert, Reg. No. 27653; Richard A. Rezek, Reg. No. 30796; Timothy E. Niednagel, Reg. No. 33266; John P. Breen, Reg. No. 38833; Jill L. Woodburn, Reg. No. 39874; Nancy J. Harrison, Reg. No. 27083; R. Trevor Carter, Reg. No. 40549;

Dilip A. Kulkarni, Reg. No. 27540; Peter Palan, Reg. No. 26213; Mark M. Newman, Reg. No. 31472; Bobby B. Gillenwater, Reg. No. 31405; Paul B. Hunt, Reg. No. 37154; Michael S. Gzybowski, Reg. No. 32816; Gerard T. Gallagher, Reg. No. 39679; and Robert D. Null, Reg. No. 40746, as attorneys of record with full power of substitution and revocation, to prosecute this application, and to transact all business in the Patent and Trademark Office connected therewith, and I specify that communications regarding the application be directed to:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
Telephone (317) 236-1313

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Jordan J. GLOGAU
Full Name of Sole or First Joint Inventor

United States of America (US)
Country of Citizenship

Inventor's Signature

Aug. 30, 1998
Date

271 Treetop Circle

Nanuet, New York 10954 NY
Residence and Post Office Address

Edward J. DELP III
Full Name of Second Joint Inventor, if any

United States of America (US)
Country of Citizenship

Second Inventor's Signature

Date

400 Evergreen Street

West Lafayette, Indiana 47906 IA
Residence and Post Office Address

Raymond B. WOLFGANG
Full Name of Third Joint Inventor, if any

United States of America (US)
Country of Citizenship

Third Inventor's Signature

Date

404 Longwood Drive

Exton, Pennsylvania 19341 PA
Residence and Post Office Address

Eugene Ted LIN
Full Name of Fourth Joint Inventor, if any

United States of America (US)
Country of Citizenship

Fourth Inventor's Signature

Date

3303 Hunter Road

West Lafayette, Indiana 47906 IA
Residence and Post Office Address

Additional inventors to be similarly identified on attached sheet.

Express Mail No.: EM466245407US

Attorney Docket No.: 3220-P-97064.00.US

DECLARATION AND POWER OF ATTORNEY – PATENT APPLICATION

As a below named inventor, I hereby declare that I believe I am the original, first and sole inventor (*if only one name is listed below*) or an original, first and joint inventor (*if plural names are listed below*) of the subject matter which is claimed and for which a patent is sought in the application entitled:

DATA HIDING

specification of which (*check one*)

_____ is attached hereto

XX was filed on 21 August 1998 (21.08.98) as

United States Application Serial No. _____ or

PCT International Application No. PCT/US98/

and was amended on _____ (if applicable)

I hereby declare that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to herein.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate on which priority is claimed (as listed below) and I have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(b) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(22.08.97)

(Application Serial No.)	(Filing Date)	(Status-patented, pending, abandoned)
60/056,724	22 August 1997	Abandoned

I hereby appoint William R. Coffey, Reg. No. 24023; Jerry E. Hyland, Reg. No. 20904; Richard D. Conard, Reg. No. 27321; Steven R. Lammert, Reg. No. 27653; Richard A. Rezek, Reg. No. 30796; Timothy E. Niednagel, Reg. No. 33266; John P. Breen, Reg. No. 38833; Jill L. Woodburn, Reg. No. 39874; Nancy J. Harrison, Reg. No. 27083; R. Trevor Carter, Reg. No. 40549;

Dilip A. Kulkarni, Reg. No. 27510; Perry Palan, Reg. No. 26213; Mark M. Newman, Reg. No. 31472; Bobby B. Gillenwater, Reg. No. 31105; Paul B. Hunt, Reg. No. 37154; Michael S. Gzybowski, Reg. No. 32816; Gerard T. Gallagher, Reg. No. 39679; and Robert D. Null, Reg. No. 40746, as attorneys of record with full power of substitution and revocation, to prosecute this application, and to transact all business in the Patent and Trademark Office connected therewith, and I specify that communications regarding the application be directed to:

BARNES & THORNBURG
11 South Meridian Street
Indianapolis, Indiana 46204
Telephone (317) 236-1313

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Jordan J. GLOGAU
Full Name of Sole or First Joint Inventor

United States of America (US)
Country of Citizenship

Inventor's Signature

Date

271 Treetop Circle

Nanuet, New York 10954
Residence and Post Office Address

Edward J. DELP III
Full Name of Second Joint Inventor, if any

United States of America (US)
Country of Citizenship

Second Inventor's Signature

8/27/98
Date

400 Evergreen Street

West Lafayette, Indiana 47906
Residence and Post Office Address

Raymond B. WOLFGANG
Full Name of Third Joint Inventor, if any

United States of America (US)
Country of Citizenship

Third Inventor's Signature

August 28, 1998
Date

404 Longwood Drive

Exton, Pennsylvania 19341
Residence and Post Office Address

Eugene Ted LIN
Full Name of Fourth Joint Inventor, if any

United States of America (US)
Country of Citizenship

Fourth Inventor's Signature

August 27, 1998
Date

3303 Hunter Road

West Lafayette, Indiana 47906
Residence and Post Office Address

Additional inventors to be similarly identified on attached sheet.

67274

6/98